UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

PUBLIC CITIZEN, et al.,)
)
)
Plaintiffs,)
v.)
) **Case No. 19-986 (RDM)**
ELISABETH DEVOS, in her official capacity)
as Secretary of the U.S. Department of)
Education, et al.)
)
Defendants.)
)

MOTION TO DISMISS COMPLAINT AS MOOT

Plaintiffs' Complaint should be denied as moot because, effective June 6, 2019, the Department of Education has provided access to Public Citizen's website through its guest Wi-Fi network as well as through internal agency network. (ECF No. 16-2, Hernandez Decl. ¶ 5) Accordingly, there is no longer a case or controversy for resolution before the Court.

ARGUMENT

Plaintiffs have filed this lawsuit seeking relief under the First Amendment and Administrative Procedure Act from an alleged "decision" by the Department of Education to block access to Public Citizen's website from the Department's internal network and guest Wi-Fi network. Public Citizen alleges that, on one occasion in February 2019, one of its staff members, Mr. Llewelyn, was unable to access Public Citizen's website utilizing the Department's guest Wi-Fi network. (Compl. ¶ 13) Plaintiff also alleges that another member of Public Citizen, Mr. Halperin, had the same experience in March 2019 and that this individual has been unable to access Public Citizen's website through the Department's guest Wi-Fi network for "approximately the past year." (Compl. ¶ 16) Although perhaps implying that there was a period of time when Mr.

Halperin could access Public Citizen's website through the Department's guest Wi-Fi network, the Complaint does not specifically make that factual assertion. Nor does Mr. Halperin in his declaration accompanying the motion for preliminary injunction attest that he, in fact, had in the past successfully accessed Public Citizen's website utilizing the guest Wi-Fi network. Thus, although the Complaint speculates about an unspecified recent "decision" to block access to Public Citizen's website, the specific allegations in the Complaint do not support that speculation.

As set forth in the accompanying Hernandez Declaration, on June 4, 2019, the Department submitted a request to its vendor to grant access to Public Citizen's website. (ECF No. 16-2, Hernandez Decl. ¶ 4). Effective June 6, 2019, access to Public Citizen's website was available through the Department's internal network and its guest Wi-Fi network. (*Id.* ¶ 5) Consequently, the Complaint should be dismissed as moot. *See, e.g., In re Howard,* 2014 U.S. App. LEXIS 13380, at *3 (D.C. Cir. July 14, 2014) ("Any injunctive relief concerning appellant's student loans would be moot, as they have been discharged"); *Nat'l Parks Conservation Ass'n v. Dep't of Interior,* 794 F. Supp. 2d 39, 44 (D.D.C. 2011) ("If . . . an agency does respond to a petition, even after a suit to compel a response is filed, such a suit is rendered moot.").

"The rule against deciding moot cases forbids federal courts from rendering advisory opinions or 'deciding questions that cannot affect the rights of litigants in the case before them.'" *Hall v. CIA*, 437 F.3d 94, 99 (D.C. Cir. 2006) (citations omitted). In *Hall*, the Court dismissed as moot Hall's challenge to the agency's denial of his FOIA fee waiver request after the agency decided to release records to Hall without seeking payment from him. *Id.* Because Hall "already has 'obtained everything that [he] could recover . . . by a judgment of this court in [his] favor,'" there was no case or controversy before the Court. The Court also held that "Hall fails to undermine the government's mootness claim with his argument that the media status claim is capable of repetition, yet evading review." *Id.* Even "[a]ssuming in Hall's favor that the matter is capable of repetition," the Court "fail[ed] to see how the issue has any tendency to evade review" because "[d]enials of fee waivers do not seem inherently of such short duration that they cannot ordinarily be fully litigated before their cessation." *Id.*

Here, access to Public Citizen's website is available. Thus, Plaintiffs have obtained everything they could recover through this action and this issue – like a denial of a FOIA fee waiver – is not "inherently of such short duration" as to have "any tendency to evade review." *See id.* Thus, as in *Hall*, the exception to the mootness doctrine for cases "capable of repetition, yet evading review" is inapplicable. *See People for the Ethical Treatment of Animals v. Gittens*, 396 F.3d 416, 424 (D.C. Cir. 2005) ("But if we are wrong about the possibility of repetition, we would still find the preliminary injunction moot because we are unconvinced that if a controversy of this sort occurred again it would evade judicial review").

The "voluntary cessation" doctrine also does not preclude a dismissal on mootness grounds. "Although generally voluntary cessation of challenged activity does not moot a case, a court may conclude that voluntary cessation has rendered a case moot if the party urging mootness demonstrates that (1) 'there is no reasonable expectation that the alleged violation will recur,' and (2) 'interim relief or events have completely or irrevocably eradicated the effects of the alleged violation.'" *Nat'l Black Police Ass'n v. D.C.*, 108 F.3d 346, 349 (D.C. Cir. 1997). That is the case here.

In the accompanying Second Hernandez Declaration, the agency explains that access to Public Citizen's website on the agency's networks was not available during the period identified in the Complaint as an unintentional consequence of the agency's transition in 2017 to a different vendor for web filtering services. (Second Hernandez Decl. ¶ 5) That new web filtering service established certain categories to which web pages were sorted by operation of proprietary methods utilized by the vendor. The categories established by the vendor by default include such things as "Potentially Liable", "Adult/Mature Content", "Bandwidth Consuming", "Security Risk", "General Interest- Personal", and "General Interest - Business." The vendor also has established subcategories that its system assigns by default to each of these categories. (Second Hernandez Decl. ¶ 8)

As the vendor's promotional material explains, its filtering service "includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block." (Ex. 1 to Second Hernandez Decl. at 1) Additionally, its web filtering "ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters." (*Id.*)

The vendor's system allows the customer to designate the following actions to apply to the designated categories: "allow", "block", "monitor", "warning", or "authenticate." For instance, on the Department's networks, the "Adult/Mature Content" category is designated by the Department, as the customer, under the "block" action. Because that category is blocked, webpages sorted by the vendor's proprietary filtering system into the subcategories under "Adult/Mature Content" also are blocked. One subcategory that the vendor places by default under the "Adult/Mature Content" category is "Advocacy Organization." (Second Hernandez Decl. ¶ 9)

The agency has determined that access to Public Citizen's website on agency networks was not available during the time period at issue because Public Citizen was categorized by the operation of the vendor's proprietary filtering system as an "Advocacy Organization" and thus was blocked under the vendor's settings. (Second Hernandez Decl. ¶10) In contrast, the other public interest organizations that Public Citizen identifies as not being blocked – such as the American Civil Liberties Union and the Center for American Progress – were assigned a different category by operation of the vendor's proprietary filtering system. (Second Hernandez Decl. ¶ 11) Specifically, both of those organizations were assigned by operation of the vendor's system to the category "General Organizations" under the subcategory "General Interest – Business." (*Id.*) That "General Organizations" category is not one designated as blocked by the Department. (Second Hernandez Decl. ¶ 12)

The vendor's system affords two different ways to override the web filtering that results from the categorization of a website by the vendor's proprietary filtering system. One method manually assigns a specific website to a different category or a locally created category. The other method is "administrative override or allow blocked override." (Second Hernandez Decl. ¶ 13) Based on request by the Department on June 4, 2019, the web filtering that, by operation of the vendor's system, had assigned Public Citizen to a blocked subcategory was overriden. That override was effective by June 6, 2019, and, accordingly, Public Citizen' s website has been accessible from the Department' s guest-WiFi and internal network since that time. (Second Hernandez Decl. ¶14)

The Department's declarant, moreover, has attested that "[t]he Department will not take any action to block access to Public Citizen's website through its internal and guest-WiFi networks, except in the event of a security risk (e.g., if Public Citizen's website were hacked or otherwise compromised) or a technical issue (e.g., bandwidth consumption) that may compromise the secure and proper functioning of the Department's networks." (ECF No. 16-2, Hernandez Decl. ¶ 6)

Thus, both requirements for the non-applicability of the voluntary cessation doctrine apply here. First, the assignment of Public Citizen's website to a blocked category occurred by operation of the vendor's propriety system, but that has been overridden as it pertains to the Public Citizen website. Consequently, in light of that override, there is no reasonable expectation that the operation of the vendor's system will again assign Public Citizen to a blocked category. Second, as a result of the override, access to Public Citizen's website on agency networks has been available since June 6, 2019. Thus, the override has eradicated the effects of the prior lack of access.

Although the Department theoretically retains the power to direct the vendor to reverse the override, such speculation is not sufficient to preclude dismissal on mootness grounds. *See Nat'l Black Police Ass'n*, 108 F.3d at 349 ("the mere power to reenact a challenged law is not a sufficient basis on which a court can conclude that a reasonable expectation of recurrence exists.") Instead, there must be evidence indicating that the challenged action is likely to recur. *Id.* Here, there is no such evidence, nor is such an inference plausible from the record. *See Citizens for Responsibility & Ethics in Washington v. SEC*, 858 F. Supp. 2d 51, 62-63 (D.D.C. 2012) (observing that "[c]hanged policy need not come in the form of a formal revocation of the previous policy, as long as the assurance of discontinuation is sufficient to establish that there is no reasonable expectation that the unauthorized actions will resume" and finding that, "[w]hile

Plaintiff's brief raises concerns about the possible recurrence . . . there are no facts to suggest" such a recurrence and Plaintiff's "conjecture is insufficient" where the defendant is a government entity).[1]

This is not a situation where the Department previously directed its vendor to assign Public Citizen's website to a blocked category and then reversed that decision after litigation was commenced. To the contrary, Public Citizen's website was one of millions of web pages that were sorted into categories by the operation of the vendor's proprietary methods. At the Department's direction, the vendor has now overridden the categorization of Public Citizen's website that had resulted from the operation of the vendor's system. Under these circumstances, there is no basis for Public Citizen to suggest that there is a likelihood of these series of events recurring in a manner that would once again render Public Citizen's website inaccessible. As the D.C. Circuit has recognized previously, "'a legal controversy so sharply focused on a unique factual context' would rarely 'present a reasonable expectation that the same complaining party would be subjected to the same action again.'" *PETA v. Gittens*, 396 F.3d 416, 424 (D.C. Cir.

[1] In *Citizens for Responsibility & Ethics in Washington*, the court observed that other courts have "consistently recognized that where the defendant is a government actor—and not a private litigant—there is less concern about the recurrence of objectionable behavior." *Citizens for Responsibility & Ethics in Washington*, 858 F. Supp. 2d at 61 (citing cases); *see also America Cargo Transp. v. United States*, 625 F.3d 1176, 1180 (9th Cir. 2010) ("Cessation of the allegedly illegal conduct by government officials has been treated with more solicitude by the courts than similar action by private parties."); *Rio Grande Silvery Minnow v. Bureau of Reclamation*, 601 F.3d 1096, 1116 & n.15 (10th Cir. 2010) (citing several cases taking this approach); *Sossamon v. Texas*, 560 F.3d 316, 325 (5th Cir. 2009) ("[C]ourts are justified in treating a voluntary governmental cessation of possibly wrongful conduct with some solicitude, mooting cases that might have been allowed to proceed had the defendant not been a public entity . . . ."); *Beta Upsilon Chi Upsilon Chapter at the Univ. of Florida v. Machen*, 586 F.3d 908, 916–17 (11th Cir. 2009) ("In cases where government policies have been challenged, the Supreme Court has held almost uniformly that voluntary cessation of the challenged behavior moots the claim."); *Ammex, Inc. v. Cox*, 351 F.3d 697, 705 (6th Cir. 2003).

2005); *see also Chichakli v. Trump*, 714 Fed. Appx 1, 2 (D.C. Cir. 2017) ("The remainder of appellant's claims were rendered moot by the removal of his name from the list of individuals subject to sanctions under Executive Order 13348 and the elimination of the Order's implementing regulation. . . . The 'voluntary cessation' exception to mootness cited by appellant does not apply because there is no reasonable expectation that appellant will be subjected in the future to the same governmental actions giving rise to the claims dismissed by the district court as moot.")

CONCLUSION

For the foregoing reasons, the Complaint should be dismissed.

Respectfully submitted,

JESSI K. LIU
D.C. BAR # 472845
United States Attorney

DANIEL F. VAN HORN
D.C. BAR # 924092
Civil Chief

By: _______/s/_____________________
JEREMY S. SIMON, D.C. BAR #447956
Assistant United States Attorney
555 4th Street, N.W.
Washington, D.C. 20530
(202) 252-2528
Jeremy.simon@usdoj.gov

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

PUBLIC CITIZEN, et al.,)
)
)
Plaintiffs,)
v.)
) **Case No. 19-986 (RDM)**
ELISABETH DEVOS, in her official capacity)
as Secretary of the U.S. Department of)
Education, et al.)
)
Defendants.)
)

ORDER

Upon consideration of Defendants' Motion to Dismiss, any opposition thereto, and the entire record herein, it is this _________ day of _________ 2019,

ORDERED that Defendants' motion is **GRANTED;** and it is

FURTHER ORDERED that the Complaint is dismissed.

SO ORDERED.

____
United States District Judge

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

PUBLIC CITIZEN, *et al.*,	)	
Plaintiffs,	)	Civil Action No. 19-CV-986 (RDM)
v.	)	
ELIZABETH DEVOS, Secretary, U.S. Department of Education.	)	
Defendant.	)	

SECOND DECLARATION OF STEVEN HERNANDEZ

I, STEVEN HERNANDEZ, declare that the following statements are true:

1. I am over 21 years of age and am competent to testify on the matters set forth herein. This declaration supplements my declaration dated June 11, 2019, that was filed in the above-captioned matter.

2. I am employed as the Chief Information Security Officer and Director of Information Assurance Services in the United States Department of Education (Department). I have served in this position, in either an acting or a permanent capacity, since December 10, 2017.

3. As the Chief Information Security Officer, my position serves as the Director, Information Assurance Services (IAS) and principal advisor to the Chief Information Officer (CIO) and Deputy Chief Information Officer (DCIO). I have full responsibility for managing Information Assurance Services operations to ensure that the confidentiality/privacy, integrity, and availability of the Department's information and information resources. I am responsible for ensuring the compliance and implementation of the Federal Information Security Management Act and E-Government Act.

4. From 2007 to 2017, the Department obtained its information technology requirements under the Education Department's Utility for Communications, Applications, and Technology Environment (EDUCATE) contract. The contract was originally awarded to Perot Systems Government Services, Inc., which was subsequently purchased by Dell, Inc. and renamed Dell Services Federal Government, Inc ("DSFG"). In 2016, DSFG changed its name to NTT Data Services Federal Government, Inc.

5. In or about 2017, the Department began to acquire segments of its information technology services requirements using multiple task or delivery orders under the Portfolio of Integrated Value-Oriented Technologies (PIVOT) program. The Department's cyber security and web filtering service requirements were satisfied under the PIVOT task orders using Fortinet FortiGuard Web Filtering. As part of the new services, all existing configurations from the legacy web filters were transferred and applied to the FortiGuard Web Filtering service. By doing so, the Department retained access to websites for which an override had been granted under the previous web filtering system.

6. Based on a review of the records regarding the Department's cyber-security program, I have been able to determine the following as to the reason why access to Public Citizen's website from the Department's guest WiFi and internal network was not available during the time period referenced in the Declaration of Patrick Llewelyn dated May 22, 2019, and the Declaration of David Halperin dated May 23, 2019.

7. FortiGuard Web Filtering is a proprietary software operated by Fortinet that sorts and rates billions of web pages into several dozen categories based on a combination of proprietary methods, including text analysis, exploitation of the web structure, and human raters. *See*

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Web_Filter/FortiGuard%20Web%20Filtering%20Service.htm (the document available at this link is attached hereto as Exhibit 1).

8. As reflected on Exhibit 1, the categories to which web pages are sorted by FortiGuard are established by Fortinet by default as part of the FortiGuard Web Filtering service and include such things as "Potentially Liable", "Adult/Mature Content", "Bandwidth Consuming", "Security Risk", "General Interest – Personal", and "General Interest – Business." As reflected on Exhibit 1, Fortinet also has established subcategories that the FortiGuard system assigns by default to each of these categories. The proprietary methods that FortiGuard Web Filtering uses to sort and rate websites into the designated default categories and subcategories are not available to the Department or shared with the Department because of their proprietary nature.

9. FortiGuard Web Filtering allows the customer to designate the following actions to apply to the designated categories: "allow", "block", "monitor", "warning", or "authenticate". For instance, on the Department's networks, the "Adult/Mature Content" category is designated by the Department, as the customer, under the "block" action. Because that category is blocked, webpages sorted by the FortiGuard proprietary filtering system into the subcategories under "Adult/Mature Content" also are blocked. As reflected on Exhibit 1, one subcategory that FortiGuard places by default under the "Adult/Mature Content" category is "Advocacy Organization."

10. Following the filing of the above-captioned lawsuit, I made inquiries to determine why Public Citizen's website was not accessible on the Department's networks. Based on those

inquiries, I learned that Public Citizen was categorized by the operation of the FortiGuard proprietary filtering system as an "Advocacy Organization" and thus was blocked under FortiGuard's settings.[1] The sorting of a website (including Public Citizen's website) to a particular category, or subcategory within a category, is the result of the operation of FortiGuard's propriety filtering system, and not any action of the Department.

11. Based on the same inquiries, I also learned that the organizations listed in the May 22, 2019 declaration of Patrick Llewellyn submitted in the above-captioned litigation were categorized by the operation of FortiGuard's proprietary filtering system as follows:

Name of Organization	SubCategory/Category
American Civil Liberties Union	General Organizations/General Interest – Business
National Consumer Law Center	Business/General Interest – Business
The Project of Predatory Student Lending at the Legal Services Center of Harvard Law School	General Organizations/General Interest-Business
The Center for American Progress	General Organizations/General Interest-Business
The U.S. Chamber of Commerce	Business/General Interest - Business
The California Association of Postsecondary Schools	Education/General Interest - Personal
The Center for Responsible Lending	Finance and Banking/General Interest - Business
The Institute for College Access and Success	Education/General Interest - Personal
Washington Legal Foundation	Government and Legal Organizations/General Interest - Business

[1] The prior vendor, DSFG, also blocked access on the Department's networks to "Adult/Mature Content." However, based on my review of documents, it does not appear that "Advocacy Organization" was a default subcategory under "Adult/Mature Content" under that vendor's filtering system. *See* Exhibit 2.

12. The category "General Interest – Business" and "General Interest – Personal" are not categories that are blocked from the Department's networks.

13. Page 5 of Exhibit 1 provides a link called "Overriding FortiGuard Website Categorization." https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/Web_Filter/Overriding%20FortiGuard%20website%20categorization.htm. As reflected on the document that is accessible through that link, FortiGuard affords two different ways to override the web filtering that results from the categorization of a website by FortiGuard's proprietary filtering system. One method manually assigns a specific website to a different Fortinet category or a locally created category. The other method is "administrative override or allow blocked override."

14. Based on request by the Department on June 4, 2019, PIVOT service providers configured the Fortinet service to override the web filtering that, by operation of the FortiGuard proprietary system, had assigned Public Citizen to a blocked subcategory. That override was effective by June 6, 2019, and, accordingly, Public Citizen's website has been accessible from the Department's guest-WiFi and internal network since that time.

I declare under penalty of perjury that the foregoing is true and correct.

Executed at Washington, DC, this 28 day of June, 2019

Steven Hernandez

EXHIBIT 1

5.4 5.2 5.0 4.3 Home Video FortiGuard Fuse KB Support

Search

Home > Online Help

> Chapter 26 - Security Profiles > Web filter > FortiGuard Web Filtering Service

Web filter
Web filter concepts
Inspection Modes
FortiGuard Web Filtering Service
Overriding FortiGuard website categorization
Web Profile Overrides
SafeSearch
YouTube Education Filter
Static URL Filter
Web content filter
Advanced web filter configurations
Configuring Web Filter Profiles
Web Filter Examples

FortiGuard Web Filtering Service

FortiGuard Web Filtering is a managed web filtering solution available by subscription from Fortinet. Before you begin to use the FortiGuard Web Filtering options, verify that you have a valid subscription to the service for your FortiGate firewall.

FortiGuard Web Filtering enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filtering Service Point to determine the category of a requested web page, and then applies the security policy configured for that user or interface. FortiGuard Web Filtering service supports detection for traffic using HTTP protocol (versions 1.0, 1.1 and 2.0).

FortiGuard Web Filtering includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block. Categories may be added or updated as the Internet evolves. To make configuration simpler, you can also choose to allow or block entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.

FortiGuard Web Filtering ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filtering Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.

FortiGuard Web Filtering and your FortiGate unit

When FortiGuard Web Filtering is enabled in a web filter or a DNS filter profile, the setting is applied to all firewall policies that use this profile. When a request for a web page appears in traffic controlled by one of these firewall policies, the URL is sent to the nearest FortiGuard server. The URL category is returned. If the category is blocked, the FortiGate unit provides a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

FortiGuard Web Filtering Actions

The possible actions are:

- **Allow** permits access to the sites within the category.
- **Block** prevents access to sites within the category. Users attempting to access a blocked site will receive a replacement message explaining that access to the site is blocked.
- **Monitor** permits and logs access to sites in the category. You may also enable user quotas when enabling

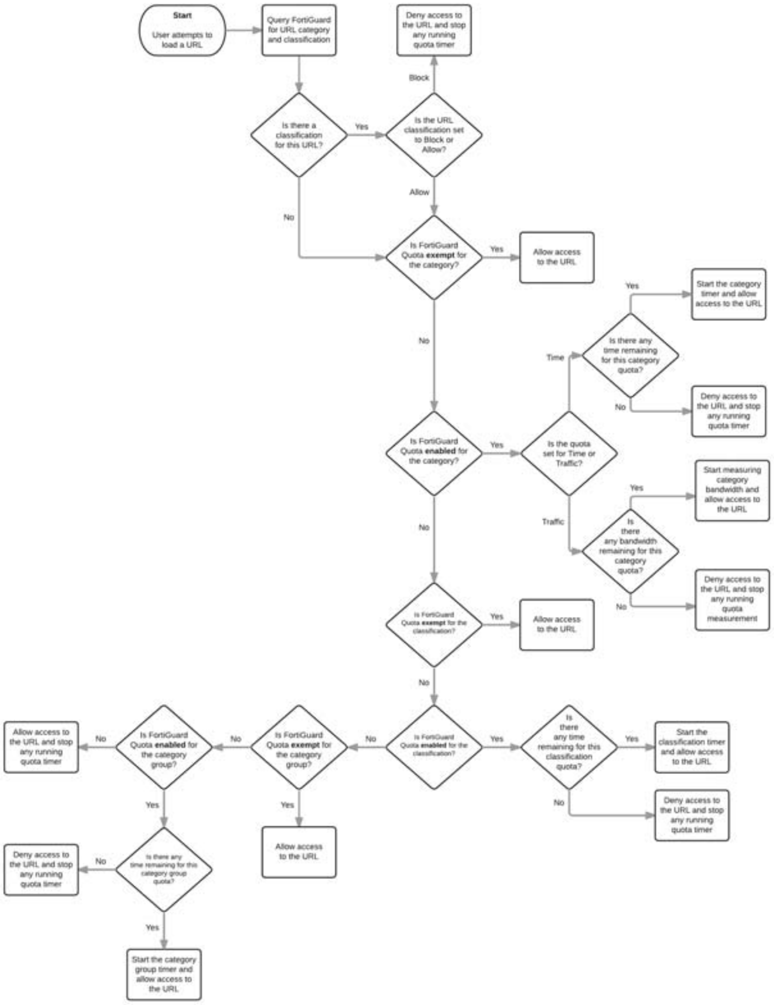
the monitor action.

- **Warning** presents the user with a message, allowing them to continue if they choose.
- **Authenticate** requires a user to authenticate with the FortiGate unit before being allowed access to the category or category group.

The options of actions available will depend on the mode of inspection.

- Proxy - Allow, Block, Monitor, Warning, Authenticate and Disable.
- Flow-based - Allow, Block & Monitor.

Web Filtering flowchart


Start
User attempts to load a URL
Query FortiGuard for URL category and classification
Deny access to the URL and stop any running quota timer
Block
Is there a classification for this URL?
Yes
Is the URL classification set to Block or Allow?
Allow
No
Is FortiGuard Quota exempt for the category?
Yes
Allow access to the URL
Yes
Start the category timer and allow access to the URL
No
Time
Is there any time remaining for this category quota?
No
Deny access to the URL and stop any running quota timer
Is FortiGuard Quota enabled for the category?
Yes
Is the quota set for Time or Traffic?
Yes
Start measuring category bandwidth and allow access to the URL
No
Traffic
Is there any bandwidth remaining for this category quota?
No
Deny access to the URL and stop any running quota measurement
Is FortiGuard Quota exempt for the classification?
Yes
Allow access to the URL
No
Allow access to the URL and stop any running quota timer
No
Is FortiGuard Quota enabled for the category group?
No
Is FortiGuard Quota exempt for the category group?
No
Is FortiGuard Quota enabled for the classification?
Yes
Is there any time remaining for this classification quota?
Yes
Start the classification timer and allow access to the URL
No
Deny access to the URL and stop any running quota timer
Yes
Yes
Allow access to the URL
Deny access to the URL and stop any running quota timer
No
Is there any time remaining for this category group quota?
Yes
Start the category group timer and allow access to the URL

FortiGuard Web Filtering categories

The following tables identify each FortiGuard web filtering category (organized by group) along with associated category IDs. For a complete description of each web filtering category, visit http://www.fortiguard.com/webfilter.

Potentially Liable

ID	Category
1	Drug Abuse

ID	Category
12	Extremist Groups

3	Hacking
4	Illegal or Unethical
5	Discrimination
6	Explicit Violence

59	Proxy Avoidance
62	Plagiarism
83	Child Abuse

Adult/Mature Content

ID	Category
2	Alternative Beliefs
7	Abortion
8	Other Adult Materials
9	Advocacy Organizations
11	Gambling
13	Nudity and Risque
14	Pornography
15	Dating

ID	Category
16	Weapons (Sales)
57	Marijuana
63	Sex Education
64	Alcohol
65	Tobacco
66	Lingerie and Swimsuit
67	Sports Hunting and War Games

Bandwidth Consuming

ID	Category
19	Freeware and Software Downloads
24	File Sharing and Storage
25	Streaming Media and Download

ID	Category
72	Peer-to-peer File Sharing
75	Internet Radio and TV
76	Internet Telephony

Security Risk

ID	Category
26	Malicious Websites
61	Phishing

ID	Category
86	Spam URLs
88	Dynamic DNS

General Interest - Personal

ID	Category
17	Advertising
18	Brokerage and Trading
20	Games
23	Web-based Email
28	Entertainment
29	Arts and Culture
30	Education
33	Health and Wellness
34	Job Search
35	Medicine
36	News and Media
37	Social Networking
38	Political Organizations
39	Reference
40	Global Religion
42	Shopping
44	Society and Lifestyles
46	Sports

ID	Category
47	Travel
48	Personal Vehicles
54	Dynamic Content
55	Meaningless Content
58	Folklore
68	Web Chat
69	Instant Messaging
70	Newsgroups and Message Boards
71	Digital Postcards
77	Child Education
78	Real Estate
79	Restaurant and Dining
80	Personal Websites and Blogs
82	Content Servers
85	Domain Parking
87	Personal Privacy
89	Auction

General Interest - Business

ID	Category
31	Finance and Banking

ID	Category
52	Information Technology

41	Search Engines and Portals	53	Armed Forces
43	General Organizations	56	Web Hosting
49	Business	81	Secure Websites
50	Information and Computer Security	84	Web-based Applications
51	Government and Legal Organizations		

Local categories

Users can define custom or local categories. See Overriding FortiGuard Website Categorization for details.

FortiGuard Web Filtering usage quotas

In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily quota by category, category group, or classification. Quotas allow access for a specified length of time or a specific bandwidth, calculated separately for each user. Quotas are reset every day at midnight.

Users must authenticate with the FortiGate unit. The quota is applied to each user individually so the FortiGate must be able to identify each user. One way to do this is to configure a security policy using the identity-based policy feature. Apply the web filter profile in which you have configured FortiGuard Web Filter and FortiGuard Web Filter quotas to such a security policy.

The use of FortiGuard Web Filtering quotas requires that users authenticate to gain web access. The quotas are ignored if applied to a security policy in which user authentication is not required.

Editing the web filter profile resets the quota timers for all users.

When a user first attempts to access a URL, they’re prompted to authenticate with the FortiGate unit. When they provide their user name and password, the FortiGate unit recognizes them, determines their quota allowances, and monitors their web use. The category and classification of each page they visit is checked and FortiGate unit adjusts the user’s remaining available quota for the category or classification.

Quota hierarchy

You can apply quotas to categories and category groups. Only one quota per user can be active at any one time. The one used depends on how you configure the FortiGuard Web Filter.

When a user visits a URL, the FortiGate unit queries the FortiGuard servers for the category of the URL. From highest to lowest, the relative priority of the quotas are:

1. Category
2. Category group

Service | Privacy Policy

Exhibit 2

Appendix H: BlueCoat Content Filter

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

Blocked Bluecoat Categories

The following Bluecoat categories are by blocked by default. Specific exceptions may be made by customer approval.

Black List

Remote Exploit

Adult/Mature Content

Child Pornography

Dynamic DNS Host

Extreme

Gambling

Games

Hacking

Intimate Apparel/Swimsuit

Malicious Outbound Data/Botnets

Malicious Sources

Nudity

Pay to Surf

Peer-to-Peer (P2P)

Personals/Dating

Phishing

Pornography

Potentially Unwanted Software

Proxy Avoidance

Scam/Questionable/Illegal

Spam

Suspicious

Violence/Hate/Racism

[redacted]